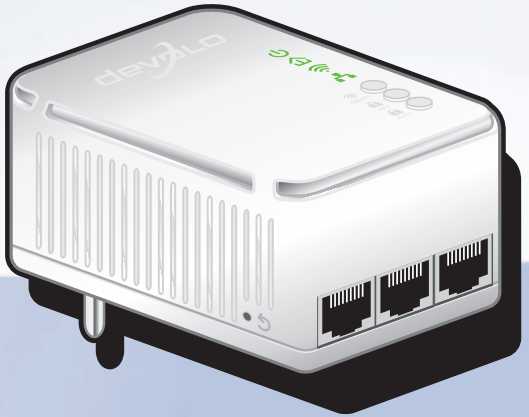
dLAN® 200 AV Wireless N



devolo dLAN® 200 AV Wireless N

© 2010 devolo AG Aachen (Germany)

While the information in this manual has been compiled with great care, it may not be deemed an assurance of product characteristics. devolo shall be liable only to the degree specified in the terms of sale and delivery.

The reproduction and distribution of the documentation and software supplied with this product and the use of its contents is subject to written authorization from devolo. We reserve the right to make any alterations that arise as the result of technical development.

Trademarks

HomePlug® is a registered trademark of HomePlug Powerline Alliance.

Linux® is a registered trademark of Linus Torvalds.

Ubuntu®is a registered trademark of Canonical Ltd.

Mac® and Mac OS X® are registered trademarks of Apple Computer, Inc.

Windows® and Microsoft® are registered trademarks of Microsoft, Corp.

Wi-Fi®, Wi-Fi Protected Access™, WPA™, WPA2™ und Wi-Fi Protected Setup™ sind eingetragene Marken der Wi-Fi Alliance®.

devolo, dLAN®, Vianect® and the devolo logo are registered trademarks of devolo AG.

The firmware package from devolo contains files which are covered by different licenses, in particular under devolo proprietary license and under open source license (GNU General Public License, GNU Lesser General Public License or FreeBSD License). The source code which is available for Open Source distribution can be requested in writing from gpl@devolo.de.

All other names mentioned may be trademarks or registered trademarks of their respective owners. Subject to change without notice. No liability for technical errors or omissions.

devolo AG

Charlottenburger Allee 60

52068 Aachen

Germany

www.devolo.com

Aachen, September 2010

Contents

1 Preface 5
1.1 Thank you! 5
1.1.1 About this manual 5

2 Introduction 7
2.1 What exactly is dLAN? 7
2.2 What is WLAN? 7
2.3 What does the adapter offer you? 8
2.4 Example application 8

3 Initial use 11
3.1 Package contents 12
3.2 System requirements 12
3.3 Functions 13
3.3.1 Control lamps 13
3.3.2 Buttons 13
3.3.3 Network jacks 15
3.3.4 WLAN antennas 15
3.4 Connecting the dLAN 200 AV Wireless N 15
3.5 Software installation 15
3.5.1 Software for Windows 15
3.5.2 Software for Mac (OS X) 1 6
3.5.3 Software for Linux (Ubuntu) 16

4 Network configuration 17
4.1 Calling up the built-in configuration interface 17
4.2 Menu description 17
4.3 Status overview 19
4.3.1 dLAN status 20
4.3.2 WLAN status 20
4.4 Device configuration 21

4.4.1 Security . . . 22
4.4.2 Network settings . . . 24
4.4.3 dLAN settings . . . 25
4.4.4 Time server . . . 26
4.5 WLAN configuration . . . 27
4.5.1 Access point . . . 29
4.5.2 WLAN filters . . . 32
4.5.3 WLAN time control . . . 34
4.5.4 Wi-Fi Protected Setup (WPS) . . . 35
4.6 Management . . . 38
4.6.1 Resetting the configuration . . . 39
4.6.2 Saving a configuration file . . . 40
4.6.3 Restoring a configuration . . . 41
4.6.4 Refresh firmware . . . 42

5 Security in the dLAN . . . 43
5.1 dLAN Cockpit . . . 43
5.1.1 Encrypting a network with dLAN Cockpit . . . 46
5.1.2 dLAN network encryption at the touch of a button . . . 47

6 Appendix. . . . 51
6.1 Important safety instructions . . . 51
6.2 Disposal of old devices . . . 52
6.3 Warranty conditions . . . 52

1 Preface

1.1 Thank you!

With the dLAN 200 AV Wireless N, you have chosen a HomePlug AV device that combines the advantages of the two network standards dLAN and WLAN. In addition, the dLAN 200 AV Wireless N has three LAN ports for directly connecting computers or other network devices. With transfer rates of up to 200 Mbps via dLAN and of up to 300 Mbps via WLAN, the dLAN 200 AV Wireless N enables wireless surfing in every room of your building—even on the other side of thick concrete walls!

1.1.1 About this manual

After a brief introduction to "dLAN" and "WLAN" basics in **Chapter 2**, **Chapter 3** will cover successfully setting up your dLAN 200 AV Wireless N. **Chapter 4** describes in detail the setting options of the built-in configuration interface and thereby also access to the WLAN. To learn what you have to do to connect your dLAN 200 AV Wireless N to dLAN, refer to **Chapter 5**. Information about product safety and environmental compatibility of the device and our warranty terms can be found in **Chapter 6** and conclude the manual.

Description of the symbols

Here we briefly describe the meaning of the symbols used in this manual.

Very important note. Failure to observe this note may result in damage.

Important note that should be observed.

Additional information, background material and configuration tips for your device.

If you have any further ideas or suggestions related to our products, we would be delighted to hear from you at support@devolo.com!

devolo on the Internet

For detailed information on our products, visit www.devolo.com. The **Service centre** area not only contains product descriptions and documentation, but also updates of devolo software and your device's firmware.

2 Introduction

dLAN is an intelligent, secure technology that lets you set up a home network easily, quickly and economically via your household electrical wiring, without the need for complex and expensive dedicated cabling. The available performance and effort required for the installation also compares favourably to traditional methods—dLAN technology now attains speeds you would expect from other LAN technologies, and installing it is a breeze!

2.1 What exactly is dLAN?

dLAN (**d**irect **L**ocal **A**rea **N**etwork) uses the household power grid to transfer data between computers equipped with suitable adapters and other network components. As a result, any power outlet can be used as a network access point. The data is modulated prior to transfer and sent as a signal via household power lines. State-of-the-art technology ensures that the power and data networks do not interfere with one another. Networking via dLAN is fast and secure. The data is encrypted using a key to prevent easy interception by third parties.

2.2 What is WLAN?

WLAN (**W**ireless **L**ocal **A**rea **N**etwork) refers to the use of radio technology to network computers and other devices. While it is possible to wirelessly connect computers in pairs (peer-to-peer, p2p), a central access point is required to set up a network of multiple devices. Such access points are frequently combined in a single device with modems for Internet access and routers to manage network traffic.

The wireless network established by an access point using a specific channel (from 1 to 13) and name (SSID) has a limited range. The range of the access point, which is also known as a "radio cell", is impeded by building walls. In some cases, stable connections are often only possible between WLAN devices within a single room.

As it is not possible to rely on hardware such as network cables (in a LAN) or household wiring (in a dLAN) to control access to a WLAN, wireless networking naturally presents special security challenges. WLANs therefore use a number of security measures, such as a concealed network name, data encryption and access control via the MAC addresses of the network adapters.

2.3 What does the adapter offer you?

With the dLAN 200 AV Wireless N, you can quickly and easily establish connections between WLAN, dLAN and LAN:

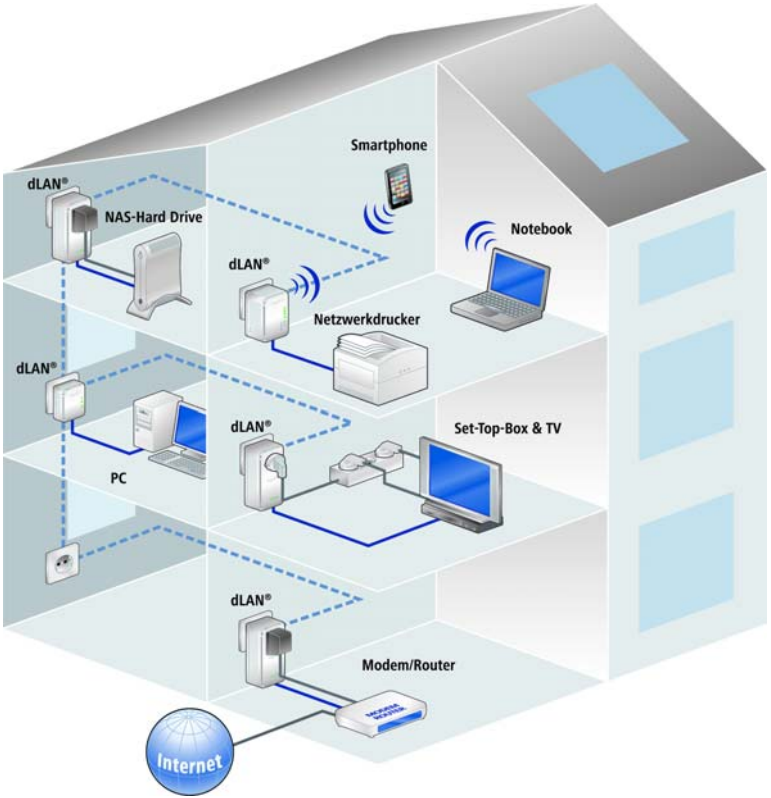
- As a WLAN access point, the adapter establishes communication between your WLAN devices and an existing LAN or dLAN network. In this way, for example, you can expand your wireless network in no time to rooms that otherwise could not be reached by wireless.
- As a dLAN device, the dLAN 200 AV Wireless N has three LAN jacks for directly connecting three network devices to the dLAN.
- By combining the LAN, dLAN and WLAN standards, you will become totally independent of existing network access points. Instead, you are completely free to connect all your devices either via a power supply socket, LAN or wirelessly. By simply reconnecting your dLAN 200 AV Wireless N, you can expand or reconfigure your home network at any time, e.g. simply by taking the adapter along into another room to work.

2.4 Example application

The dLAN 200 AV Wireless N is a WLAN access point and makes the dLAN network connected via the mains outlet available wirelessly to other client devices, such as laptops, IP radios or IP telephones.

This is particularly practical if not all client stations are within range of a WLAN access point, for example because concrete walls disrupt the signal. With dLAN, however, various rooms can be easily connected via the mains supply. And using a dLAN 200 AV Wireless N, you can quickly and easily turn every mains outlet into a WLAN connection with excellent reception quality.

The following illustration shows how the dLAN 200 AV Wireless N is used to establish a connection to the Internet and within the home network for additional dLAN 200 AV devices and a router.


Smartphone
dLAN®
NAS-Hard Drive
Notebook
dLAN®
Netzwerkdrucker
dLAN®
dLAN®
Set-Top-Box & TV
PC
dLAN®
Modem/Router
Internet

3 Initial use

This chapter covers everything you need to know to set up your dLAN 200 AV Wireless N. It will explain connecting the device and its functions. We will also briefly introduce the included devolo software and then guide you through its installation.

3.1 Package contents

Please ensure that the delivery is complete before beginning with the installation of your dLAN 200 AV Wireless N.

- **Single Kit**:
  - dLAN 200 AV Wireless N
  - Hard copy of installation guide
  - CD containing software and online documentation

or

- **Starter Kit**:
  - dLAN 200 AV Wireless N
  - dLAN 200 AVmini
  - Network cable
  - Hard copy of installation guide
  - CD containing software and online documentation

devolo AG reserves the right to change the package contents without prior notice.

3.2 System requirements

- **Operating systems**: Windows XP (32-bit), Windows Vista Home Premium (32-bit/64-bit), Windows 7 Home Premium (32-bit/64-bit), Linux (Ubuntu), Mac OS X and all operating systems with network support
- **Network connection**

Please note that your computer or other device must feature a network adapter with a network port.

Please note that dLAN devices such as the devolo dLAN duo (14 Mbps) and devolo dLAN 85 HSmini (85 Mbps) can be used on the same mains supply as dLAN 200 AV devices (200 Mbps) without interference, but they will not be able to communicate directly with one another. To set up a dLAN 200 AV network, you need at least two dLAN 200 AV devices (200 Mbps). More valuable information about dLAN or dLAN 200 AV is available in the Service Centre section of our website at www.devolo.com***.***

3.3 Functions

The dLAN 200 AV Wireless N has the following elements:

3.3.1 Control lamps

Power

Green: Lit steady when the dLAN 200 AV Wireless N is operational.

dLAN

Green: The network connection is suitable for HD video streaming; flashes when data is being transmitted.

Orange: The network connection is suitable for SD video streaming and online gaming; flashes when data is being transmitted.

Red: The network connection is suitable for simple data transfer and Internet access; flashes when data is being transmitted.

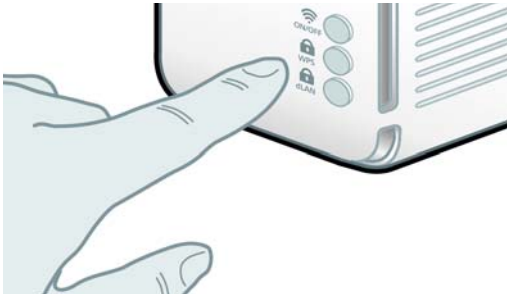
WLAN

Green: Lit steady when a connection to the WLAN network exists; flashes when data is being transmitted.

Ethernet

Green: Lit steady when a connection to the Ethernet network exists; flashes when data is being transmitted.

3.3.2 Buttons



ON/OFF

Use the ON/OFF button to switch the **WLAN** function on or off.

Make sure that the WLAN function in the factory defaults is enabled and the WLAN encryption is set to WPA2. The standard WLAN key is the security ID of the dLAN 200 AV Wireless N. You will

find the 16-character security ID on the label on the back of the housing.

WPS

With the WPS (**W**i-Fi **P**rotected **S**etup) encryption button, you secure your WLAN network at the touch of a button.

WPS is one of the encryption standards developed by the Wi-Fi Alliance for increasing security in a WLAN home network. The objective of WPS is to make it easier to add devices to an existing network. For more detailed information, refer to Chapter **4.5.4 Wi-Fi Protected Setup (WPS)**.

dLAN

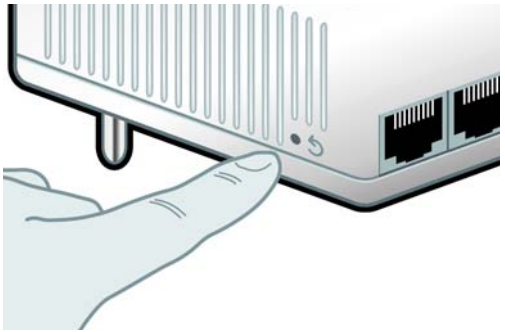
Via the dLAN encryption button, you secure your dLAN network at the touch of a button:

- To encrypt your dLAN 200 AV network individually, press **each encryption button on the connected devices** for approx. **1 second** – within 2 minutes.
- To remove a dLAN 200 AV device from your network, press the **encryption button** of the corresponding device **for at least 10 seconds**.

For more details on dLAN encryption, refer to Chapter **5 Security in the dLAN**.

Reset

The **Reset** button (on the side of the housing) has two different functions:



- **The device restarts** if you press the Reset button **for less than 10 seconds**.
- To change the configuration of the dLAN 200 AV Wireless N back to the **factory defaults**, press the Reset button **for more than 10 seconds**. Keep in mind that all settings that have already been configured will be lost!

The reset button can be pressed using the tip of a ball-point pen.

3.3.3 Network jacks

The three LAN ports can be used to connect computers or other network devices to the dLAN 200 AV Wireless N via commercially available network cables.

3.3.4 WLAN antennas

The internal WLAN antennas are for connecting to other network devices wirelessly.

3.4 Connecting the dLAN 200 AV Wireless N

This section describes how to connect your dLAN 200 AV Wireless N to a computer or other network device.

① Use a network cable to connect the dLAN 200 AV Wireless N to the network port of your running computer or other network device.

② Plug the dLAN 200 AV Wireless N into a wall socket.

③ Once you have connected at least two dLAN 200 AV adapters as described above, your dLAN 200 AV network has been set up. To secure your network **individually**, continue with the configuration. To do so, read further in Chapter **4 Network configuration** and **5 Security in the dLAN**.

3.5 Software installation

3.5.1 Software for Windows

Use the installation wizard to install the devolo software for using the adapter with the Windows operating system:

- devolo **dLAN Cockpit** finds all reachable dLAN adapters in your dLAN 200 AV network, displays information about these devices and encrypts your dLAN 200 AV network individually.
- Configure your WLAN network via the built-in **configuration interface** of your dLAN 200 AV Wireless N.

To install the software, insert the included CD-ROM in the CD drive of your computer. If autoplay is installed on your computer, the installation will start automatically. Otherwise, open the folder with the Windows Explorer by right-clicking on **Start** and selecting **Explorer** from the context menu. Double-click to start the installation wizard manually.

During the installation process, you will be given the choice of installing all software components (**Standard installation**) or selecting individual ones (**Custom installation**).

To take full advantage of the functions of your device, we recommend installing all of the applications.

You will be asked for permission to transfer anonymous performance data related to your dLAN adapter to devolo. The data sent to devolo pertains only to the performance values of your dLAN devices. The data is anonymised and will be used exclusively for statistical purposes. By providing it, you can help us improve our products. You can find the installed software applications in the **Start** ▷ **All Programs** ▷ **devolo** program group.

3.5.2 Software for Mac (OS X)

The **software** ▷ **mac** folder contains the dLAN configuration software.

3.5.3 Software for Linux (Ubuntu)

The **software** ▷ **linux** folder contains the dLAN configuration software.

4 Network configuration

The dLAN 200 AV Wireless N has a built-in configuration interface that can be called up using a standard web browser. Most settings for operating the device can be modified here. To integrate the dLAN 200 AV Wireless N into an existing dLAN network for the first time only, use the **dLAN Cockpit** or the **encryption button** (see Chapter **5 Security in the dLAN**).

4.1 Calling up the built-in configuration interface

Call up the built-in online configuration interface of the dLAN 200 AV Wireless N using the dLAN Cockpit program under **Start** ▷ **All Programs** ▷ **devolo** ▷ **Cockpit**. Open the **Configuration page of the adapter** by moving the mouse pointer over the tab of the dLAN 200 AV Wireless N.

Then the program determines the current IP address and starts the configuration in the web browser.

By default, you will come directly to the configuration interface. However, if a login password was set up via the option **Device configuration** ▷ **Security**, *you have to enter it first. Read more about this under* **4.4.1 Security**.

4.2 Menu description

Thanks to the logical menu structure, the configuration interface is user-friendly and intuitive to operate. All menu functions are described in the corresponding interface as well as in the associated chapter in the manual. The sequence of the description in the manual follows the structure of the menu.

Click **Save** to save the settings of the respective area of the configuration interface. Click **Back** to leave the respective area of the configuration interface.

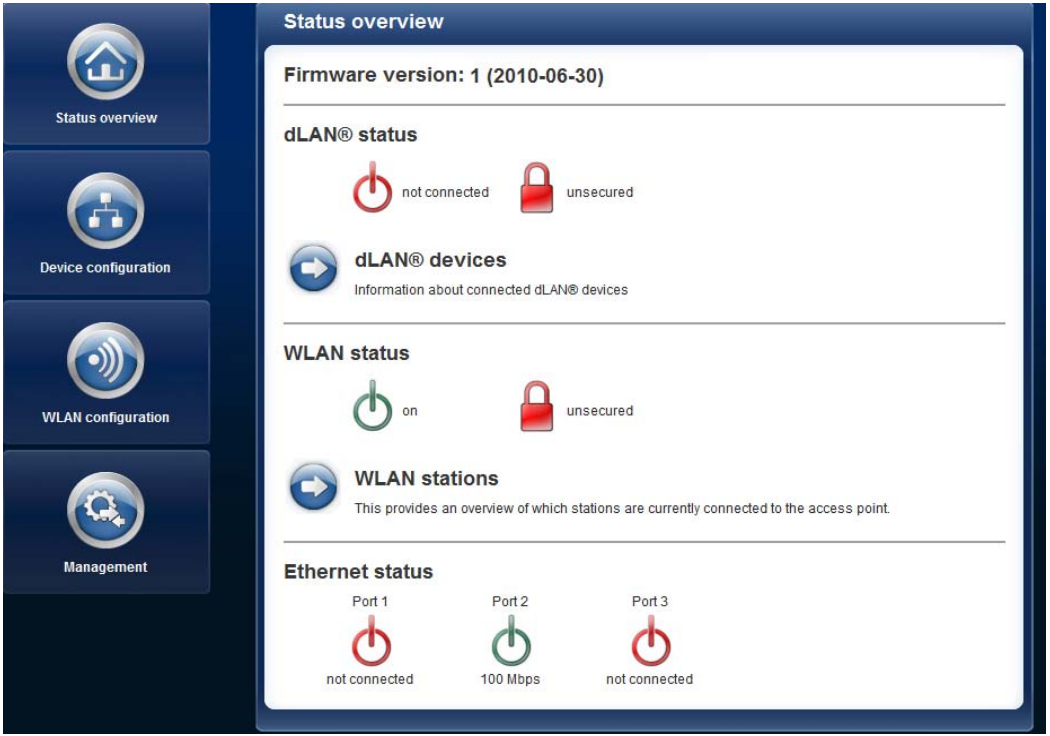
Select the desired language in the language selection list.

At first, after starting the configuration interface, the four central areas are displayed:

- In the **Status overview** area, you get general information about all connected dLAN, WLAN and LAN devices.
- You can change or modify the various settings for your device under **Device configuration**.
- You can change or modify WLAN settings in the **WLAN configuration** area.
- The **Management** section is for resetting, securing and restoring your individual configurations. In addition, you can update the firmware of your dLAN 200 AV Wireless N here.

4.3 Status overview

In the **Status overview** area you can track the status of your connected dLAN, WLAN and LAN devices.

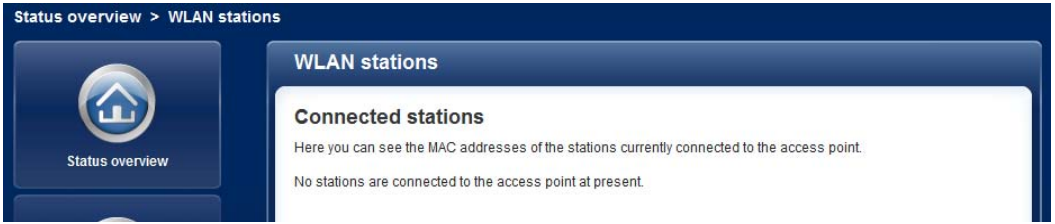


4.3.1 dLAN status

To display all connected dLAN devices, click either the **Ready to operate** icon or the **dLAN devices** arrow. Each connected dLAN device, regardless of whether it is connected locally or in the network, is displayed with its MAC address. Clicking the **lock** icon brings you directly to the **dLAN settings** (see **4.4.3 dLAN settings**).

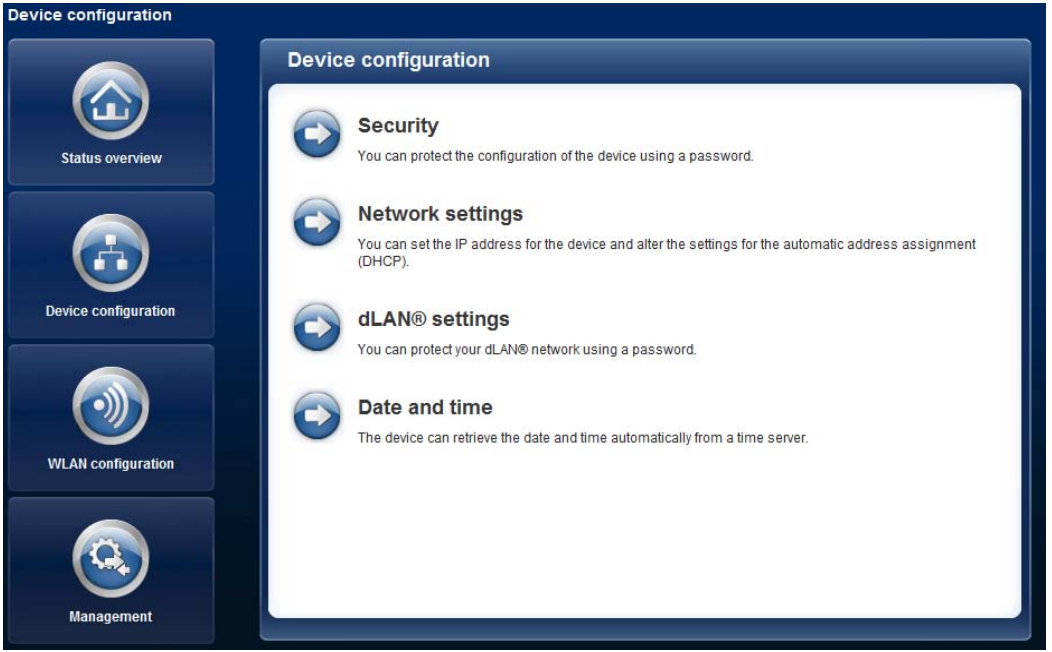
4.3.2 WLAN status

To display all connected WLAN devices, click either the **Ready to operate** icon or the **WLAN stations** arrow. Each connected WLAN client is displayed with its MAC address. Clicking the **lock** icon brings you directly to the **WLAN filters** area (see **4.5.2 WLAN filters**), where you can configure settings for network security.


Status overview > WLAN stations
Status overview
WLAN stations
Connected stations
Here you can see the MAC addresses of the stations currently connected to the access point.
No stations are connected to the access point at present.

4.4 Device configuration

In the configuration area you can modify settings for security, network, dLAN, date and time.


Device configuration
Status overview
Device configuration
WLAN configuration
Management
Device configuration
Security
You can protect the configuration of the device using a password.
Network settings
You can set the IP address for the device and alter the settings for the automatic address assignment (DHCP).
dLAN® settings
You can protect your dLAN® network using a password.
Date and time
The device can retrieve the date and time automatically from a time server.

4.4.1 Security

In this area you can set a login password for access to the configuration interface of the dLAN 200 AV Wireless N.

By default, the built-in configuration interface of the dLAN 200 AV Wireless N is not protected with a password. After installing the dLAN 200 AV Wireless N, however, you should enable this protection by assigning a password to prevent access by a third party.

To do so, first enter (if present) the current password and then enter the desired new password twice. Now the configuration interface is protected against unauthorised access with your individual password!

If the configuration interface is called up again later, the following window appears first:

Windows Security
The server 169.254.21.210 at . requires a username and password.
Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).
admin
Remember my credentials
OK
Cancel

Enter **admin** in the **User name** field and your individual password in the **Password** field.

The admin ***user name cannot be changed.***

4.4.2 Network settings

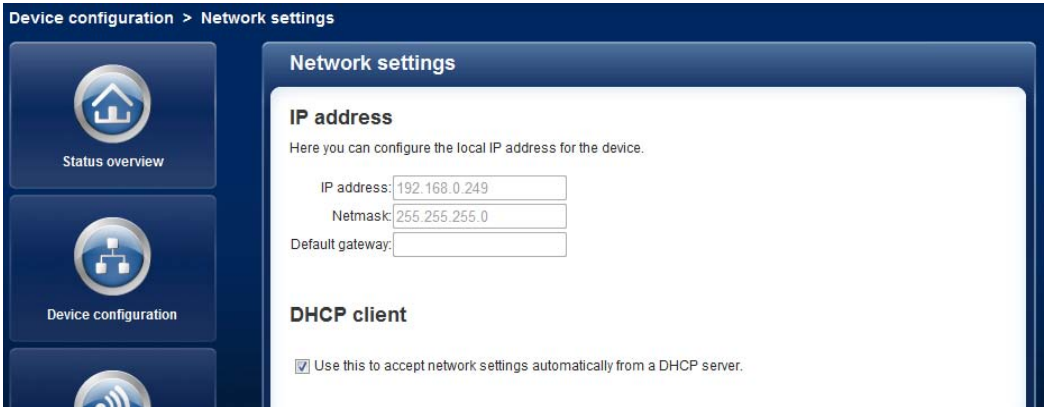
The dLAN 200 AV Wireless N also communicates via the TCP/IP protocol as a component of your home network. The IP address required for this can either be entered manually as a static address or obtained **automatically** from a **DHCP server**.

The option **Use this to accept network settings automatically from a DHCP server** is enabled in the factory defaults.

If a DHCP server is already present in the network for giving out IP addresses, have the option **Use this to accept network settings automatically from a DHCP server** enabled so that the dLAN 200 AV Wireless N automatically receives an address from it.

You can also assign a static IP address by making entries under **IP address** (e.g. '192.168.0.250') and **Netmask** (e.g. 255.255.255.0).

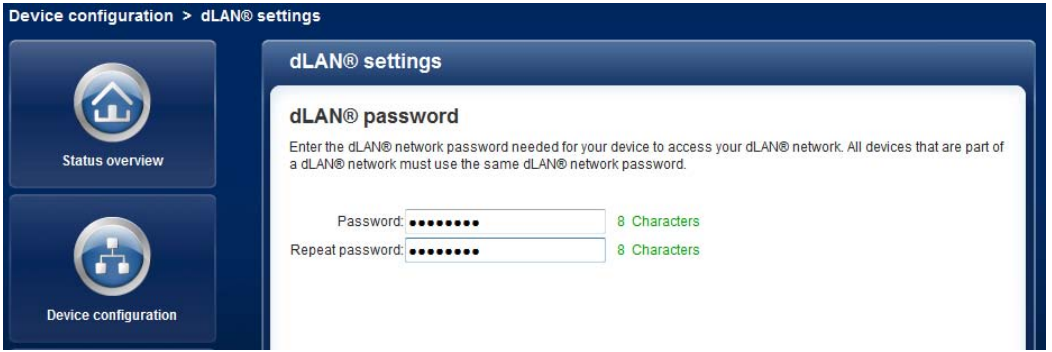
If you ever forget the IP address of your dLAN 200 AV Wireless N, open the **dLAN Cockpit** *to find the device in the network. Proceed as described under* **4.1 Calling up the built-in configuration interface**.


Device configuration > Network settings
Status overview
Device configuration
Network settings
IP address
Here you can configure the local IP address for the device.
IP address: 192.168.0.249
Netmask: 255.255.255.0
Default gateway:
DHCP client
Use this to accept network settings automatically from a DHCP server.

4.4.3 dLAN settings

In a dLAN network, all connected components must use the same password. The dLAN password is normally defined once at the installation of your dLAN 200 AV Wireless N using the dLAN Cockpit or the dLAN encryption button (see Chapter **5 Security in the dLAN**) or is taken over from the existing network.

The dLAN standard password is* HomePlugAV*.

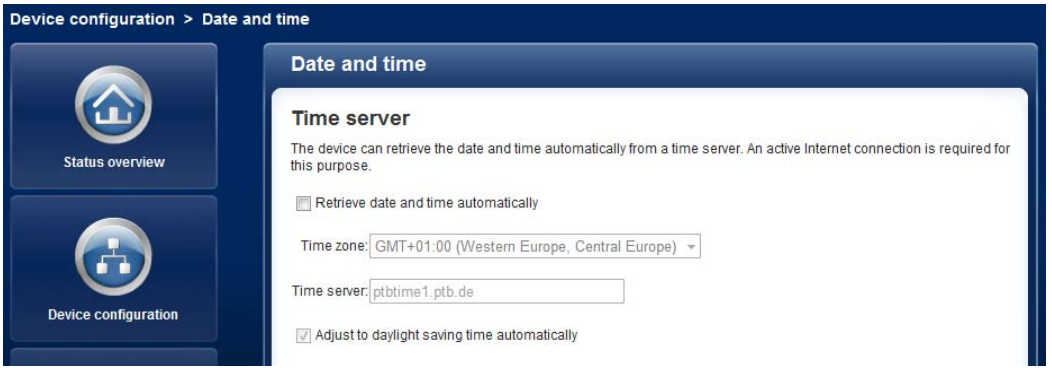

Device configuration > dLAN® settings
Status overview
Device configuration
dLAN® settings
dLAN® password
Enter the dLAN® network password needed for your device to access your dLAN® network. All devices that are part of a dLAN® network must use the same dLAN® network password.
Password:
8 Characters
Repeat password:
8 Characters

4.4.4 Time server

A time server is a server on the Internet whose task consists of providing the exact time. Most time servers are coupled with a radio clock.

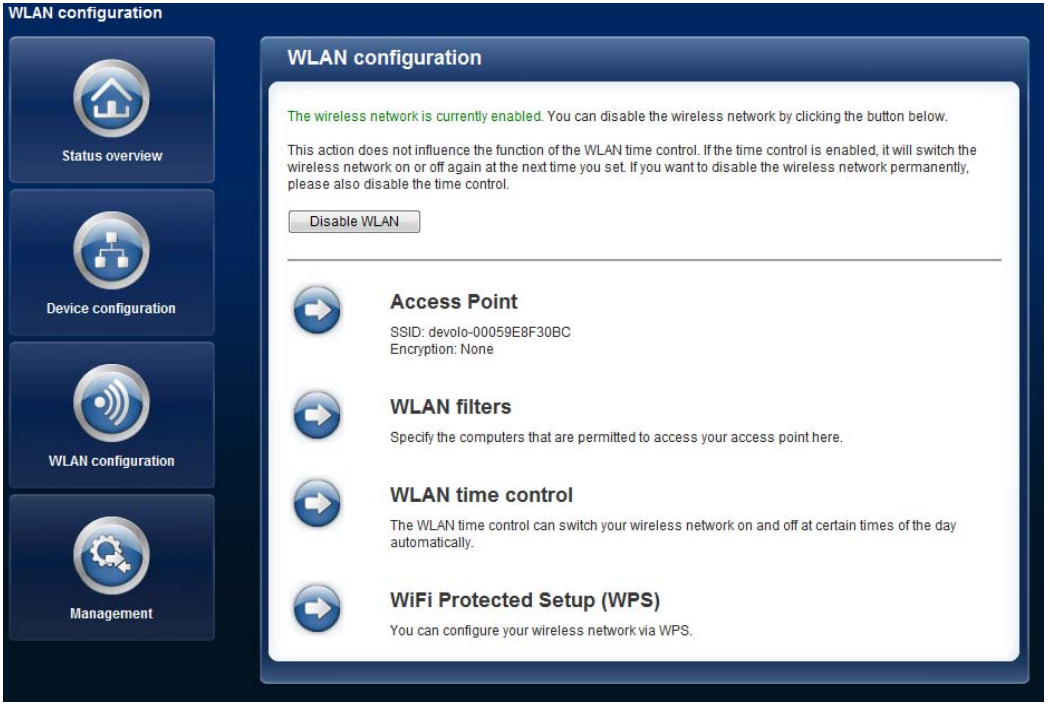
To see which Internet time server your computer uses to communicate, simply click the clock in the lower right corner of the screen and select the **Internet time** *tab.*

Enable the option **Retrieve date and time automatically**, so that the dLAN 200 AV Wireless N can automatically synchronise the date and time. Select your **Time zone** and the **Time server**. If you have enabled the option **Adjust to daylight saving time automatically**, the dLAN 200 AV Wireless N automatically adjusts to daylight saving time.


Device configuration > Date and time
Status overview
Device configuration
Date and time
Time server
The device can retrieve the date and time automatically from a time server. An active Internet connection is required for this purpose.
Retrieve date and time automatically
Time zone: GMT+01:00 (Western Europe, Central Europe)
Time server: ptbtime1.ptb.de
Adjust to daylight saving time automatically

4.5 WLAN configuration

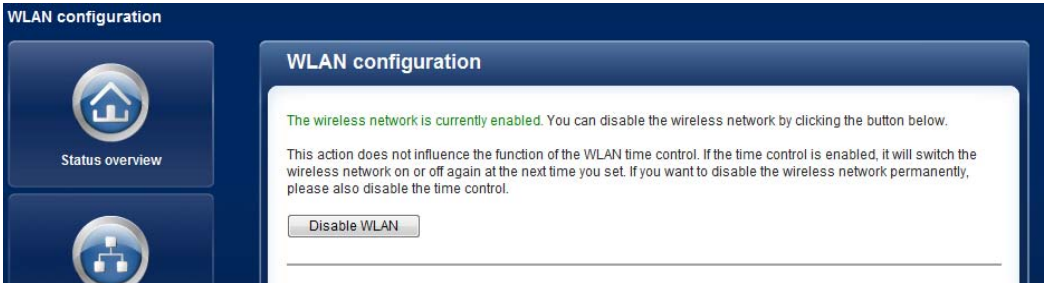
In the **WLAN configuration** area, you can configure settings for the WLAN network and its security.


WLAN configuration
Status overview
Device configuration
WLAN configuration
Management
WLAN configuration
The wireless network is currently enabled. You can disable the wireless network by clicking the button below.
This action does not influence the function of the WLAN time control. If the time control is enabled, it will switch the wireless network on or off again at the next time you set. If you want to disable the wireless network permanently, please also disable the time control.
Disable WLAN
Access Point
SSID: devolo-00059E8F30BC
Encryption: None
WLAN filters
Specify the computers that are permitted to access your access point here.
WLAN time control
The WLAN time control can switch your wireless network on and off at certain times of the day automatically.
WiFi Protected Setup (WPS)
You can configure your wireless network via WPS.

There are three different methods for switching the **WLAN function** on and off:

- Simply press the **ON/OFF button** on the front panel of the device.
- Use the **Enable WLAN** or **Disable WLAN** button on the configuration interface under **WLAN configuration**.
- Enable the WLAN time control. For more information, refer to Chapter **4.5.3 WLAN time control**.

The operating state of the device is displayed under **4.3 Status overview**.


WLAN configuration
Status overview
WLAN configuration
The wireless network is currently enabled. You can disable the wireless network by clicking the button below.
This action does not influence the function of the WLAN time control. If the time control is enabled, it will switch the wireless network on or off again at the next time you set. If you want to disable the wireless network permanently, please also disable the time control.
Disable WLAN

4.5.1 Access point

Since the dLAN 200 AV Wireless N acts as an access point, you have to configure various parameters for your wireless network. If you would like, you can completely shut off the WLAN part of your dLAN 200 AV Wireless N, e.g. if you want to operate it exclusively as a simple dLAN device via the built-in Ethernet connections. To do so, switch off the **Enable WLAN** option under **Status overview** ⇨ **WLAN stations**, or simply press the **WLAN ON/OFF** button on the housing.

Keep in mind that after saving this setting, you will be disconnected from any existing wireless connection to the dLAN 200 AV Wireless N. In this case, configure the device via Ethernet or dLAN.

When activating the encryption, make sure that the WLAN settings (SSID, encryption mode and encryption key) of the access point always correspond to the settings of the clients, as otherwise you will be (unintentionally) excluding devices from your network.

In the factory defaults ***of the dLAN 200 AV Wireless N, the*** WLAN function is enabled ***and the*** WPA2 ***WLAN encryption is set with the*** security ID as the standard WLAN key***. You will find the 16-character security ID on the label on the back of the housing.***

For operation as an access point, a (transmission) channel must be specified. There are 13 channels available. We recommend keeping the default setting **Auto**, since in this setting the dLAN 200 AV Wireless N selects the channel regularly and independently. In other words, if the last connected station logs out, a

search for a suitable channel is carried out immediately. If no stations are connected, the device automatically selects a channel every 15 minutes.

The **SSID** specifies the name of your wireless network. You can see this name when logging onto the WLAN and thereby identify the correct subnet. If you enable the **Hide SSID** option, your wireless network remains hidden. In this case, potential network users must know the exact SSID and enter it manually to be able to set up a connection.

Some WLAN adapters have difficulty connecting to such hidden wireless networks. If the connection to a hidden SSID poses problems, first try to set up the connection with a visible SSID and only then try to hide it.

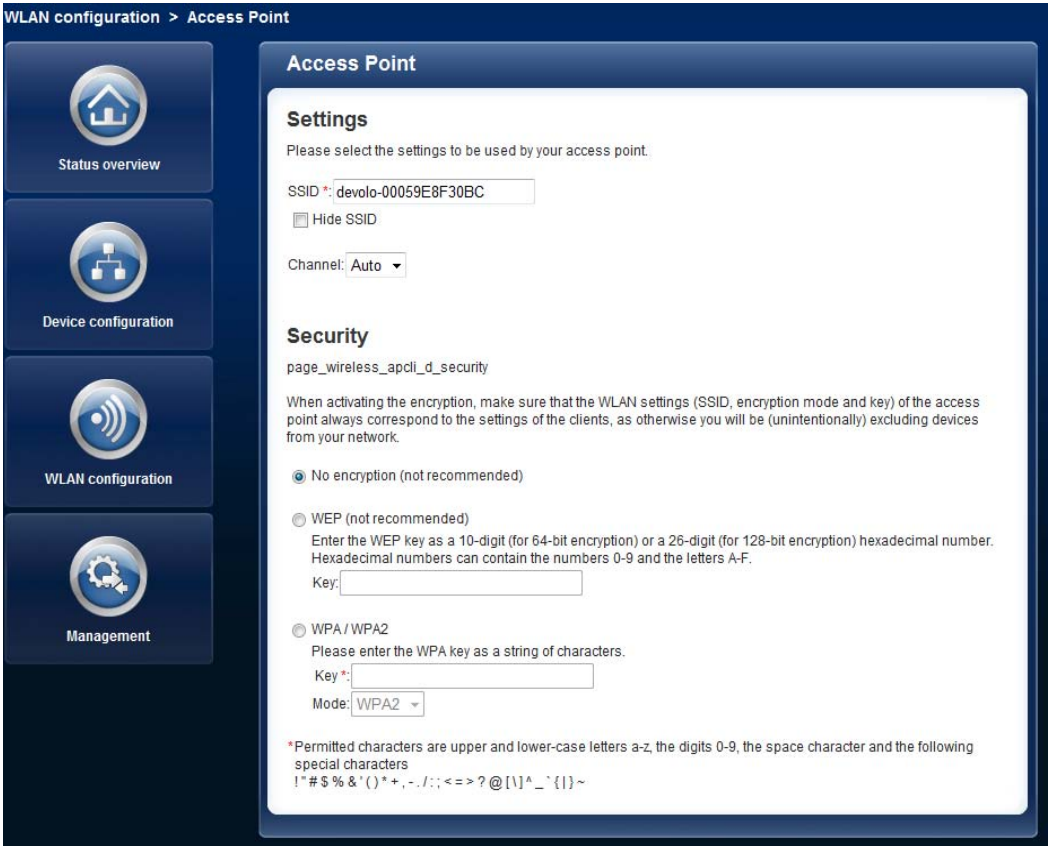
Without encryption, not only are all data transmitted from client computers to the dLAN 200 AV Wireless N in your wireless network without protection, but there is also no password prompt to establish the connection. If no other security measures were set up, such as a WLAN filter (see Chapter **4.5.2 WLAN filters**), third parties can gain access to your network at any time and, for example, share your Internet connection. Usually this happens without you noticing it.

To secure the data transmission in your wireless network there are two security standards available.

- The older and weaker **WEP** standard can protect communication with the help of a key having either **10 or 26 characters**. To do so, enter a series of hexadecimal characters with the corresponding number of characters into the **Key** field.
- The state-of-the-art **WPA and WPA2 (Wi-Fi Protected Access)** methods allow individualised keys consisting of **letters and numbers with a length of up to 63 characters**. You can simply enter this using the keyboard, without having to convert it into hexadecimal format first (as with WEP). Under **Mode**, you can limit access of clients to the dLAN 200 AV Wireless N to the method you have selected.

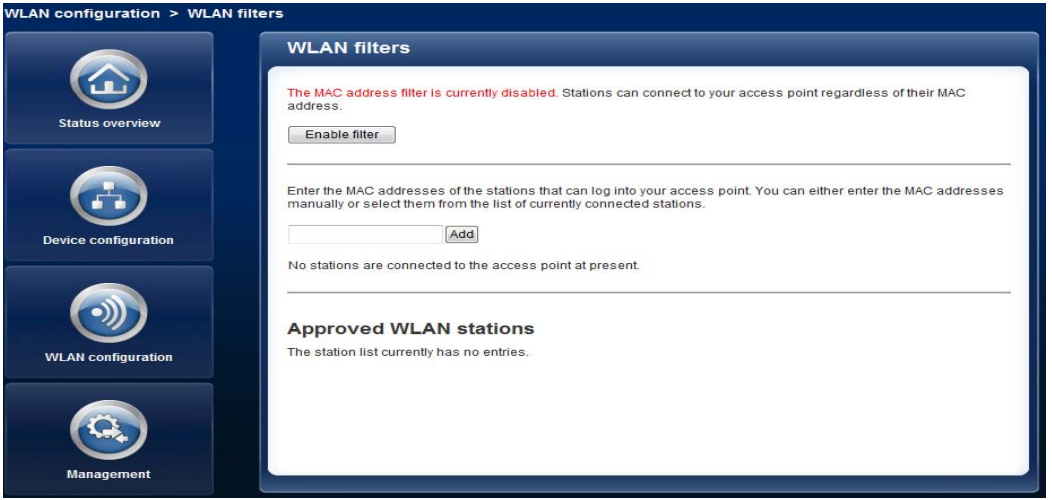
Save all modified settings before leaving this configuration area again.

You should always encrypt the connections in your WLAN. Otherwise anyone within range could penetrate into your home network and, for example, share your Internet connection. Always select the better WPA2 encryption method if possible. Use WEP only if one of your wireless terminal devices does not operate with a better standard.


WLAN configuration > Access Point
Status overview
Device configuration
WLAN configuration
Management
Access Point
Settings
Please select the settings to be used by your access point.
SSID *: devolo-00059E8F30BC
Hide SSID
Channel: Auto
Security
page_wireless_apcli_d_security
When activating the encryption, make sure that the WLAN settings (SSID, encryption mode and key) of the access point always correspond to the settings of the clients, as otherwise you will be (unintentionally) excluding devices from your network.
No encryption (not recommended)
WEP (not recommended)
Enter the WEP key as a 10-digit (for 64-bit encryption) or a 26-digit (for 128-bit encryption) hexadecimal number. Hexadecimal numbers can contain the numbers 0-9 and the letters A-F.
Key:
WPA / WPA2
Please enter the WPA key as a string of characters.
Key *:
Mode: WPA2
*Permitted characters are upper and lower-case letters a-z, the digits 0-9, the space character and the following special characters
! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~

4.5.2 WLAN filters

In addition to encryption (see **4.5.1 Access point**), you can secure your wireless network even more by using a WLAN filter to limit access via WLAN to the dLAN 200 AV Wireless N for selected devices. Even if the encryption is switched off, the device will not establish a connection.


WLAN configuration > WLAN filters
Status overview
Device configuration
WLAN configuration
Management
WLAN filters
The MAC address filter is currently disabled. Stations can connect to your access point regardless of their MAC address.
Enable filter
Enter the MAC addresses of the stations that can log into your access point. You can either enter the MAC addresses manually or select them from the list of currently connected stations.
Add
No stations are connected to the access point at present.
Approved WLAN stations
The station list currently has no entries.

The WLAN filter should be used only as an additional option. By using it you could limit access to your wireless network, but without encryption it would be relatively easy for third parties to eavesdrop on all of your data transmissions.

To use the WLAN filter, enable the option **Enable filters**. Now you can enter various network devices by means of what is known as your MAC address for access to your dLAN 200 AV Wireless N. Confirm each entry with **Add**. Network devices or stations connected to your dLAN 200 AV Wireless N are automatically listed, that is, to enable an already connected station for the dLAN 200 AV Wireless N, simply select the MAC address of the respective device and confirm it with **Add**. This then appears under **Approved WLAN stations**. To remove an enabled station, select its MAC address and confirm it with **Delete**.

The MAC address designates the hardware interface of each individual network device uniquely (e.g. the WLAN adapter of a computer or the Ethernet port of a printer). It consists of six double-digit hexadecimal numbers, each separated by a colon (e.g. 00:0B:3B:37:9D:C4). The MAC address is on the housing of the device.

You can easily determine the MAC address of a Windows computer by opening the window with the command prompt under **Start** ▷ **All Programs** ▷ **Accessories** ▷ **Command Prompt**. Enter the command **IPCONFIG /ALL** here. The MAC address is displayed under the designation **Physical address**.

After entering the MAC addresses, do not forget to click the **Save** button. If the entered values are incorrect (e.g. because the colons are missing), a corresponding error message is displayed.

Keep in mind that you also have to enter the MAC address of your own computer if you are connected to the dLAN 200 AV Wireless N not via the Ethernet port, but via WLAN. Otherwise you will block your own access to the device via WLAN by activating the WLAN filter!

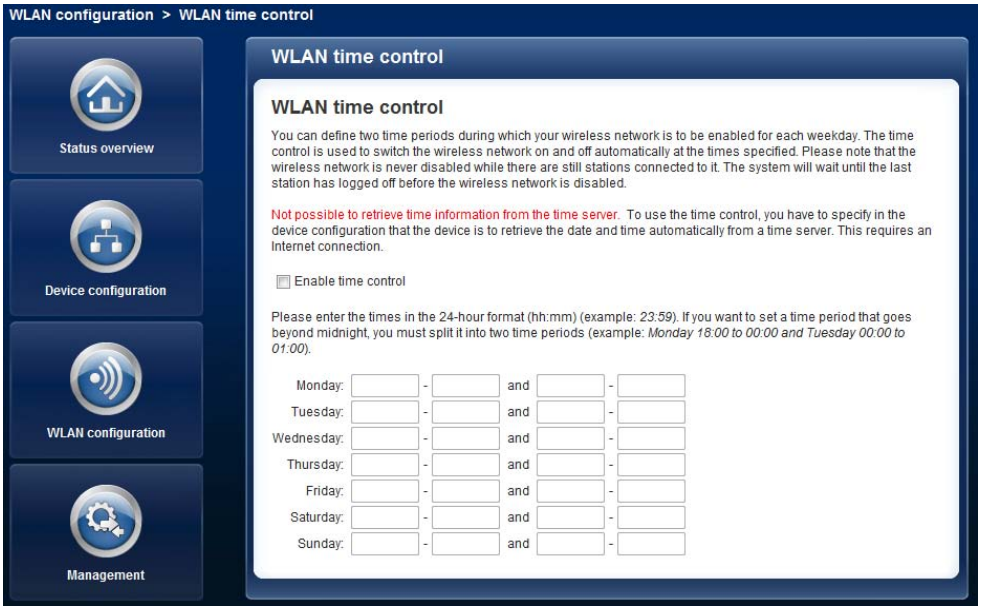
4.5.3 WLAN time control

To be able to use the WLAN time control, the option Retrieve date and time automatically must be enabled under Device configuration ⇨ Date and time***. An active Internet connection is also required. (see*** 4.4.4 Time server***)***

To be able to use the WLAN time control, enable the option **Enable time control**. The time control automatically switches your wireless network on and off at certain times of the day.

You can define two time periods during which your wireless network is to be enabled for each weekday. Then the time control automatically switches the wireless network on or off.

Keep in mind that, as long as the dLAN 200 AV Wireless N registers connected stations, the wireless network remains enabled. The wireless network is not switched off until the last station has logged off.


WLAN configuration > WLAN time control
Status overview
Device configuration
WLAN configuration
Management
WLAN time control
WLAN time control
You can define two time periods during which your wireless network is to be enabled for each weekday. The time control is used to switch the wireless network on and off automatically at the times specified. Please note that the wireless network is never disabled while there are still stations connected to it. The system will wait until the last station has logged off before the wireless network is disabled.
Not possible to retrieve time information from the time server. To use the time control, you have to specify in the device configuration that the device is to retrieve the date and time automatically from a time server. This requires an Internet connection.
Enable time control
Please enter the times in the 24-hour format (hh:mm) (example: 23:59). If you want to set a time period that goes beyond midnight, you must split it into two time periods (example: Monday 18:00 to 00:00 and Tuesday 00:00 to 01:00).
Monday: - and -
Tuesday: - and -
Wednesday: - and -
Thursday: - and -
Friday: - and -
Saturday: - and -
Sunday: - and -

4.5.4 Wi-Fi Protected Setup (WPS)

Wi-Fi Protected Setup (WPS) is one of the international encryption standards developed by the Wi-Fi Alliance for easily and quickly setting up a secure wireless network. The encryption keys of the respective WLAN client are transmitted automatically and continuously to the other WLAN client(s) of the wireless network. The dLAN 200 AV Wireless N offers two different variants for transmitting these encryption keys:

WPS via PBC (Push Button Configuration):

① Start the encryption process on the dLAN 200 AV Wireless N

- ○ either by pressing the **WPS button** on the **front panel of the device** or
- ○ by pressing the **Start setup** button on the user interface under **WLAN configuration** ▷ **Wi-Fi Protected Setup (WPS)**.

② Then press either the WPS key of the WLAN client you are adding or the WPS button on the configuration interface. Now the devices exchange their encryption keys and establish a secure WLAN connection. The WLAN LED on the front panel indicates the synchronisation process by flashing.

WPS via PIN:

① To interconnect WLAN clients securely in your wireless network via PIN variants, enter an individualised key in the configuration interface under **WLAN configuration** ▷ **Wi-Fi Protected Setup (WPS)** ▷ **PIN** and start the encryption process by pressing the **Start setup** button.

② Open the configuration interface of the WLAN client to be added and transmit the PIN selected on the dLAN 200 AV Wireless N. Confirm the encryption process as described there. Now the devices exchange their encryption keys and establish a secure WLAN connection. The WLAN LED on the front panel indicates the synchronisation process by flashing.

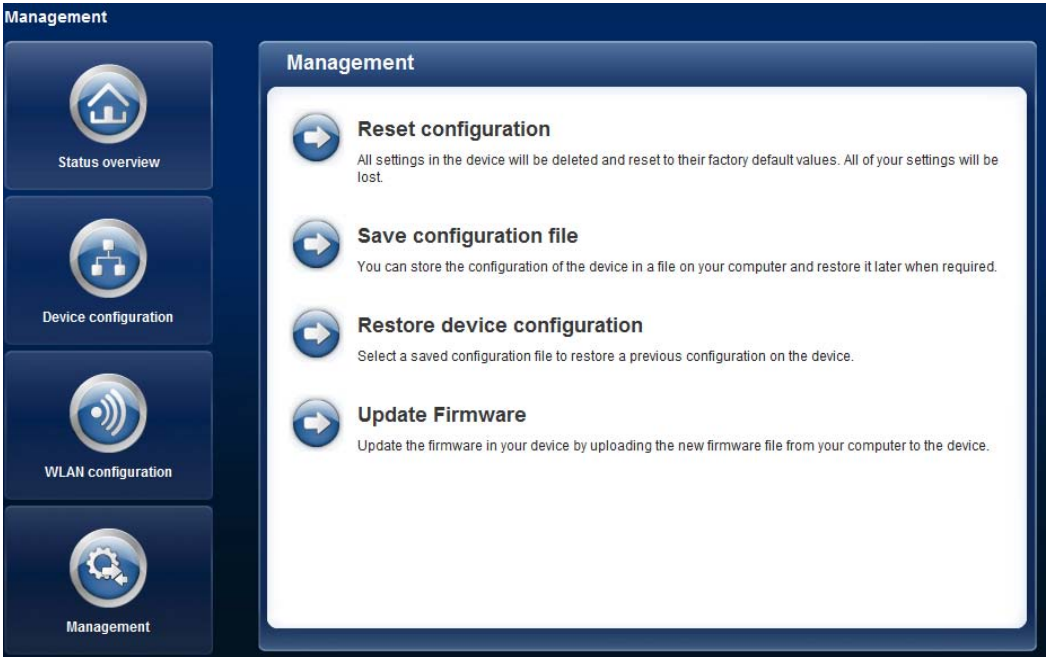
WLAN configuration > WiFi Protected Setup (WPS)
Status overview
Device configuration
WiFi Protected Setup (WPS)
WPS via PBC (Push Button)
The WPS configuration can be started either via the WPS button on the device or via the web interface. Please start the configuration process and then press the WPS button on the station that is to join into the wireless network.
Start setup
WPS via PIN
The device also supports WPS via a PIN. In order to join a station into your wireless network via PIN, please enter the PIN and then start the configuration process. Next, you must tell your station that it should join into the wireless network. The PIN of the station is usually either printed on the housing or specified on the configuration interface.
PIN:
Start setup

Use of the **WPS** process implies either **WPA** or **WPA2**. For that reason, keep in mind the following automatic settings depending on the encryption standard (also refer to **4.5.1 Access point**), i.e.

- if under **WLAN configuration** ⇨ **Access Point** **No encryption** or **WEP** is selected in advance, **WPA2** is set automatically. The newly generated password is displayed under **WLAN configuration** ⇨ **Access Point** in the **Key** field.
- if under **WLAN configuration** ⇨ **Access Point** **WEP** is selected in advance, **WPA2** is set automatically. The newly generated password is displayed under **WLAN configuration** ⇨ **Access Point** in the **Key** field.
- if under **WLAN configuration** ⇨ **Access Point** **WPA** is selected in advance, this setting remains with the previously assigned password.
- if under **WLAN configuration** ⇨ **Access Point** **WPA2** is selected in advance, this setting remains with the previously assigned password.

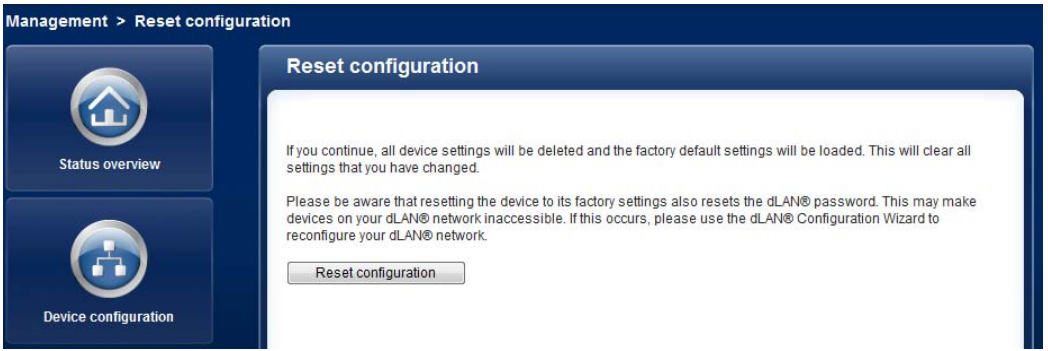
4.6 Management

In the **Management** area you can reset the current configuration to the factory defaults, save it to your computer as a file or restore it from there and update the firmware of the dLAN 200 AV Wireless N.


Management
Status overview
Device configuration
WLAN configuration
Management
Management
Reset configuration
All settings in the device will be deleted and reset to their factory default values. All of your settings will be lost.
Save configuration file
You can store the configuration of the device in a file on your computer and restore it later when required.
Restore device configuration
Select a saved configuration file to restore a previous configuration on the device.
Update Firmware
Update the firmware in your device by uploading the new firmware file from your computer to the device.

4.6.1 Resetting the configuration

With the **Management** ▷ **Reset configuration** command, the dLAN 200 AV Wireless N is reset to the original factory defaults. In doing so, you lose your personal settings. The last-assigned dLAN password for the dLAN 200 AV Wireless N is also reset to the dLAN standard password **HomePlugAV**. To secure your dLAN 200 AV network individually again, reconfigure it by using either the encryption button or the dLAN Cockpit (see **5 Security in the dLAN**).

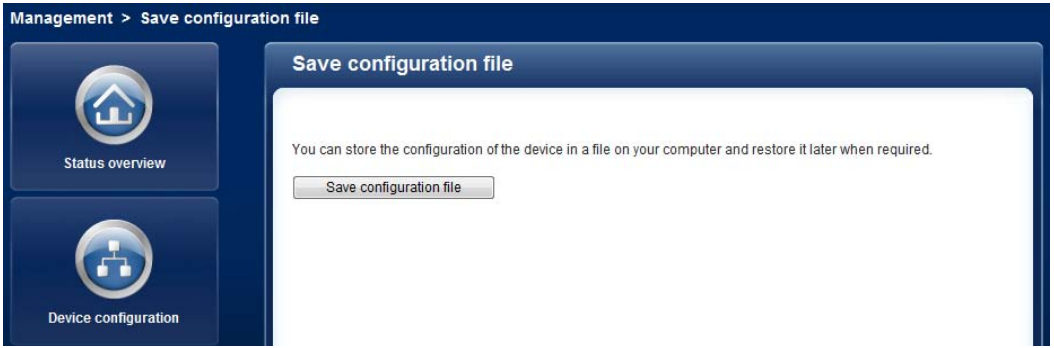

Management > Reset configuration
Status overview
Device configuration
Reset configuration
If you continue, all device settings will be deleted and the factory default settings will be loaded. This will clear all settings that you have changed.
Please be aware that resetting the device to its factory settings also resets the dLAN® password. This may make devices on your dLAN® network inaccessible. If this occurs, please use the dLAN® Configuration Wizard to reconfigure your dLAN® network.
Reset configuration

You can change the dLAN password by using the dLAN Cockpit in the Windows program group Start ▷ All Programs ▷ devolo ***or by using the encryption button.***

For backup purposes, all active configuration settings can be transmitted to your computer, stored there as a file and reloaded into the dLAN 200 AV Wireless N. In this way, you can for example generate configurations for different network environments, with which you can set up the device quickly and easily.

4.6.2 Saving a configuration file

To save the active configuration to your computer as a file, select the corresponding button in the area **Management** ▷ **Save configuration file**. Then enter a storage location and name for the settings file.


Management > Save configuration file
Status overview
Device configuration
Save configuration file
You can store the configuration of the device in a file on your computer and restore it later when required.
Save configuration file

4.6.3 Restoring a configuration

An existing configuration file can be sent to the dLAN 200 AV Wireless N in the area **Management** ◊ **Restore device configuration** and enabled there. Select a suitable file via the **Browse…** button and start the operation by clicking the **Restore device configuration** button.

4.6.4 Refresh firmware

The firmware of the dLAN 200 AV Wireless N includes the software for operating the device. If necessary, devolo offers new versions on the Internet as a file download, for example to modify existing functions.

① To bring the firmware up to the latest version, first go to the devolo website, www.devolo.com, and download the appropriate file for the dLAN 200 AV Wireless N to your computer.

② Then in the configuration dialogue, go to the area **Management** ⇨ **Update Firmware**. Click **Browse…** and select the downloaded file.

③ Then start the update procedure with the **Update Firmware** button. After a successful update, the dLAN 200 AV Wireless N restarts.

Ensure that the update procedure is not interrupted. To do so, it is best to connect your computer to the dLAN 200 AV Wireless N via dLAN or LAN rather than WLAN.

5 Security in the dLAN

Before you can use the dLAN 200 AV Wireless N in your dLAN network, first you have to connect it to other dLAN 200 AV devices as a home network. Two specific pieces of information are especially important for this:

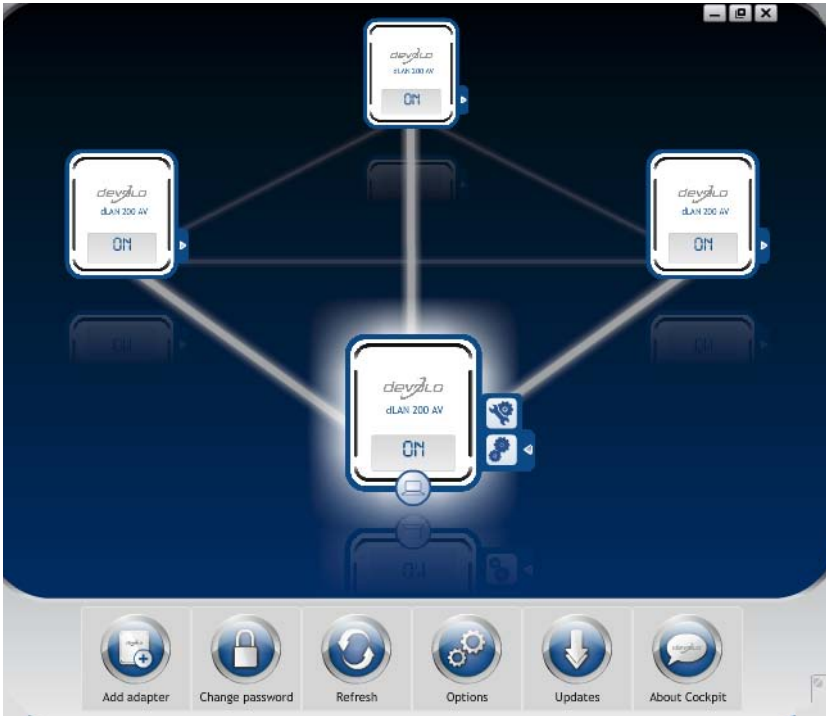
- Shared use of a dLAN password results in a delimited dLAN network.
- Shared use of the dLAN password serves as access control to the dLAN network as well as the encryption, and thereby the interception protection, of the transmitted data.

The dLAN password can be specified automatically via the **encryption button** or manually using the **dLAN Cockpit** program. Please note the following basic principle when choosing your encryption method:

- In dLAN 200 AV networks, data encryption is as **simple as touching a button**, since **all corresponding dLAN 200 AV devices are equipped with an encryption button**.
- For dLAN 200 AV networks that include devices **with and without encryption buttons**, data encryption must be set up using the **dLAN Cockpit**.

5.1 dLAN Cockpit

devolo **dLAN Cockpit** is a monitoring and encryption program that detects all reachable dLAN 200 AV devices in your home network and combines them in a secure network. Due to its logical graphic design, the dLAN Cockpit is easy and intuitive to operate. After installing the devolo software, it can be found in the **Start** ⇨ **Programs** ⇨ **devolo** program group.



After starting the dLAN Cockpit, the locally connected dLAN 200 AV adapter will be searched for and displayed first. Then all other reachable dLAN devices in your home network will appear. This may take a moment.

All adapters found in the network appear with as adapter icon with a corresponding product name. The adapter in the middle of the dLAN network identified with the symbol shown here symbolises your locally connected device. If you have multiple dLAN devices connected locally, you can jump back and forth between them. Clicking an adapter icon with the mouse enables the corresponding dLAN 200 AV device and highlights it.

The coloured connecting lines of the adapters illustrate the current transmission quality:

- **Green**: the network connection is suitable for HD video streaming.
- **Orange**: the network connection is suitable for SD video streaming and online gaming.
- **Red**: the network connection is suitable for simple data transfer and Internet access.

If data transmission from one device to another is actually taking place, the data rate is displayed on the respectively highlighted adapter.

Settings and functions

You can configure settings for the respectively highlighted device or for the network

- via the buttons at the bottom edge of the screen
- or via tabs arranged at the side of each adapter.

You can always use the **Refresh** button to display the current status of devices that have been found (if this hasn't happened automatically).

By means of the **Options** button or the corresponding tabs of the respective adapter, you can learn device information such as the firmware version used and the individual MAC address.

Options are given like assigning an **additional name**, resetting the respective device to the **factory default settings** or **removing** a **device** from the existing dLAN network.

The above-mentioned setting options vary depending on the function and features of your device.

You can also specify whether information on the performance of your dLAN adapters will be transferred to devolo.

The data sent to devolo pertains only to the performance values of your dLAN devices. The data is anonymised and will be used exclusively for statistical purposes. By providing it, you can help us improve our products.

The **Troubleshooting Guide** includes installation instructions and information about how to connect your devices optimally with one another.

5.1.1 Encrypting a network with dLAN Cockpit

If you use dLAN 200 AV devices **without an encryption button**, data can be encrypted only via **dLAN Cockpit**.

Before the networking procedure, note the security IDs of all dLAN 200 AV adapters. This unique identifier of each dLAN device is located on the label on the housing. It consists of 4 x 4 letters separated by dashes (e.g. ANJR-KMOR-KSHT-QRUV). Ensure that all dLAN adapters are connected to the power grid and computers or other network components as appropriate.

Scan for local adapter

After dLAN Cockpit is started, it searches for the dLAN adapter connected directly to your computer first.

Adding an adapter

Add all the dLAN devices you want to your dLAN network by selecting the **Add adapter** button. You will need the **16**-character security IDs of the adapters from the label on the housing. Enter it now in the **Security ID** field and confirm with **OK**. If a security ID is correct and the device can be reached in the dLAN network, it will be added to your network of configured adapters and also displayed in the program.

Entering a network password

After you have added all the dLAN devices you want to your dLAN network, select the **Change password** button to assign a shared network password that will apply for all registered adapters in your personal home network.

You can choose between your own password, a random password and the default password. To define your own password with a length of at least eight characters, enter this into the **Network password** (min. 8 characters) text field. Alternatively, you can have a randomly selected, highly secure password assigned using the **Generate secure password** button. Use the **Factory default password** button to reset the dLAN adapter to the default password. Normally, the display of the password is hidden for security reasons. If you enable the option **Show characters**, the current password is displayed in legible form in the text field.

The factory default password is* HomePlugAV*. Assigning a specific password to a single adapter will exclude it from the remaining dLAN network.

If **dLAN Cockpit** is called up again later after a successful initial installation, for example to **integrate** a **new adapter** into a network, the application remembers the devices that were entered earlier. Enter the new device as described in the **Adding an adapter** section. The **current network password** is assigned **automatically** to the newly added device.

5.1.2 dLAN network encryption at the touch of a button

To encrypt a dLAN 200 AV network, in which all associated devices are equipped with an encryption button, simply press the encryption button that is located on the device. Pressing this button will encrypt your dLAN 200 AV network with a randomly generated password.

The following section contains exact instructions on the basis of possible network scenarios:

Encrypting a new network with a dLAN 200 AV Wireless N and a dLAN 200 AVmini (Fig. 1)

Once both adapters have been successfully connected, press each encryption button **for approx. one second within two minutes of one another**.

That's it! Your dLAN 200 AV network is now protected against unauthorised access.

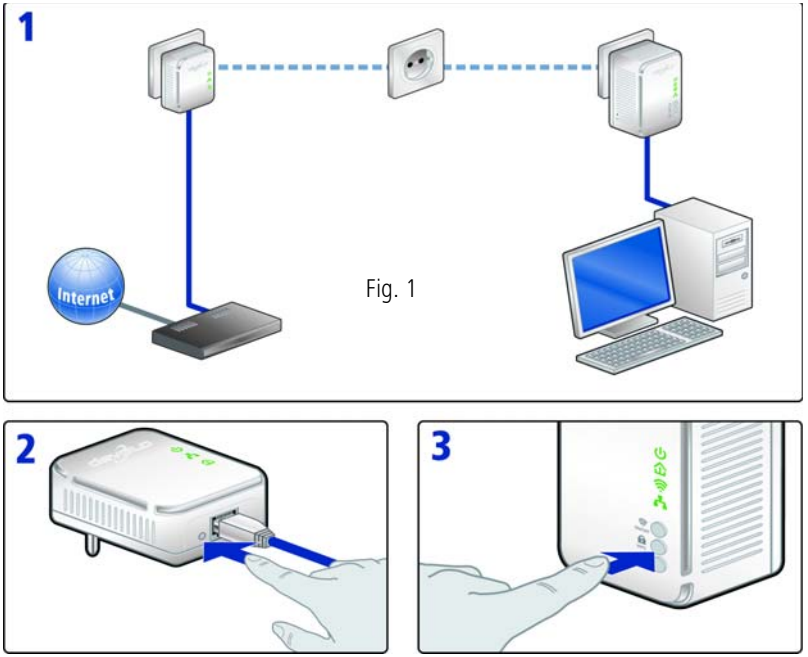


Fig. 1

Expanding an existing dLAN 200 AV network by adding a new dLAN 200 AV Wireless N (Fig. 2)

If you have already secured your existing dLAN 200 AV network using the encryption button, use the same method to integrate further adapters. Once you have successfully connected the new dLAN 200 AV Wireless N, first press the encryption button (approx. **one second**) of one of your network's existing adapters, then press the encryption button (approx. **one second**) of your new dLAN 200 AV Wireless N **within two minutes**.

That's it! The new dLAN 200 AV Wireless N is now integrated in your network. To integrate additional adapters in your network, repeat the above steps.

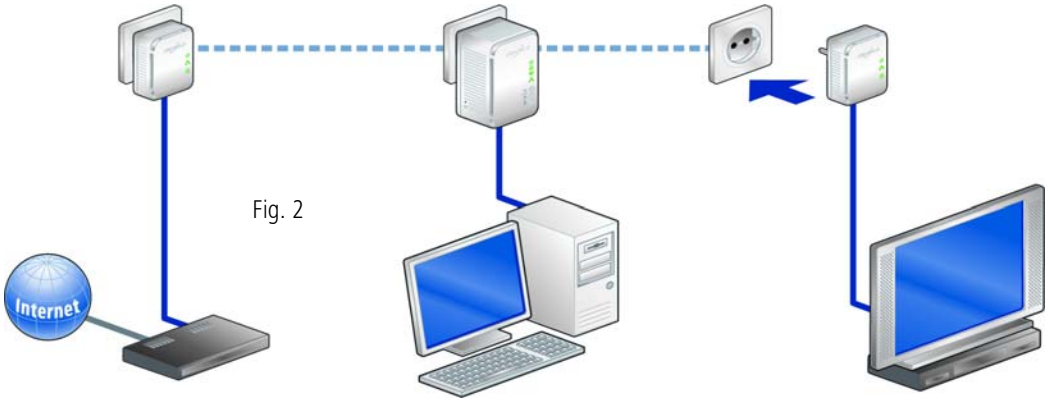


Fig. 2

Removing a dLAN 200 AV Wireless N from a network (Fig. 3)

To remove a dLAN 200 AV Wireless N adapter from an existing network, press its encryption button for **at least 10 seconds**. The device will be assigned a new randomly generated password and will thus no longer be able to access the network. To integrate the device into a different dLAN 200 AV network, follow the steps described above, depending on whether you are setting up a new network or adding the adapter to an existing one.

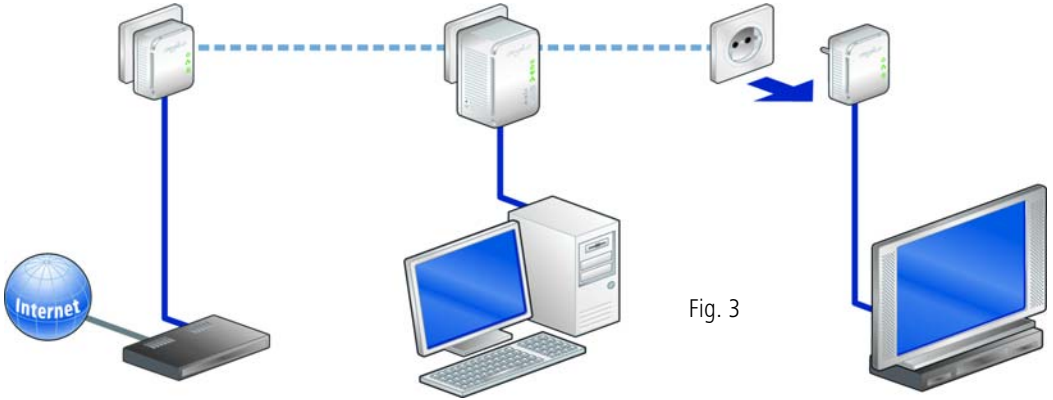


Fig. 3

6 Appendix

For the permitted voltage range for operating the device and the power consumption, refer to the label on the rear side of the device.

For the CE declaration for this product, refer to the accompanying product CD under CE*. Additional technical information is available at* www.devolo.com.

6.1 Important safety instructions

All safety and operating instructions should be read and understood before using the device, and should be kept for future reference.

- Never open the device. There are no user-serviceable parts inside the device.

Do not try to service this product yourself! Contact qualified technicians each and every time your device needs maintenance. There is a risk of electric shock!

- Use the device in a dry location only.
- Always use the included network cable to connect the device.
- Do not insert any objects into the openings of the device.
- To disconnect the device from the power supply grid, pull the power plug.
- Do not keep the device in direct sunlight.
- Slots and openings on the case serve as ventilation. Never block or cover them.
- Never set up the device near a heater or radiator.
- The device should be located only where sufficient ventilation can be ensured.
- Disconnect the device from the power supply grid before cleaning. Use a moist towel to clean the device. Never use water, paint thinner, benzene, alcohol or other strong cleaning agents when cleaning the device, as these could damage the case.
- Never use the device with a power supply that does not meet the specifications provided on the rating plate. If you do not know what type of power supply you have at home, contact your dealer or energy supplier.
- In the event of damage, disconnect the device from the power supply grid and contact customer service. This applies, for example, if
  - the power cable or plug is damaged.

- liquid has been spilled on the device or objects have fallen into the device.
- the device has been exposed to rain or water.
- the device does not work, even though the operating instructions have been followed properly.
- the device's case is damaged.

6.2 Disposal of old devices

The icon with crossed-out wastebasket on the device means that this adapter is an electrical or electronic device that falls within the scope of application of the German Electrical and Electronic Equipment Act. Since 24 March 2006, these types of devices may no longer be disposed of with household waste. Rather, in Germany, they can be given to a municipal collection point free of charge. Contact your municipal government to find out the address and hours of the nearest collection point.

6.3 Warranty conditions

The devolo AG warranty is given to purchasers of devolo products in addition to the warranty conditions provided by law and in accordance with the following conditions:

1 Warranty coverage

a) The warranty covers the equipment delivered and all its parts. Parts will, at devolo's sole discretion, be replaced or repaired free of charge if, despite proven proper handling and adherence to the operating instructions, these parts became defective due to fabrication and/or material defects. Alternatively, devolo reserves the right to replace the defective product with a comparable product with the same specifications and features. Operating manuals and possibly supplied software are excluded from the warranty.

b) Material and service charges shall be covered by devolo, but not shipping and handling costs involved in transport from the buyer to the service station and/or to devolo.

c) Replaced parts become property of devolo.

d) devolo is authorized to carry out technical changes (e.g. firmware updates) beyond repair and replacement of defective parts in order to bring the equipment up to the current technical state. This does not result in any additional charge for the customer. A legal claim to this service does not exist.

2 Warranty period

The warranty period for this devolo product is three years. This period begins at the day of delivery from the devolo dealer. Warranty services carried out by devolo do not result in an extension of the warranty period nor do they initiate a new warranty period. The warranty period for installed replacement parts ends with the warranty period of the device as a whole.

3 Warranty procedure

a) If defects appear during the warranty period, the warranty claims must be made immediately, at the latest within a period of 7 days.

b) In the case of any externally visible damage arising from transport (e.g. damage to the housing), the person carrying out the transportation and the sender should be informed immediately. On discovery of damage which is not externally visible, the transport company and the sender are to be immediately informed in writing, at the latest within 3 days of delivery.

c) Transport to and from the location where the warranty claim is accepted and/or the repaired device is exchanged, is at the purchaser's own risk and cost.

d) Warranty claims are only valid if a copy of the original purchase receipt is returned with the device. devolo reserves the right to require the submission of the original purchase receipt.

4 Suspension of the warranty

All warranty claims will be deemed invalid

a) if the label with the serial number has been removed from the device,

b) if the device is damaged or destroyed as a result of acts of nature or by environmental influences (moisture, electric shock, dust, etc.),

c) if the device was stored or operated under conditions not in compliance with the technical specifications,

d) if the damage occurred due to incorrect handling, especially to non-observance of the system description and the operating instructions,

e) if the device was opened, repaired or modified by persons not contracted by devolo,

f) if the device shows any kind of mechanical damage, or

g) if the warranty claim has not been reported in accordance with 3a) or 3b).

5 Operating mistakes

If it becomes apparent that the reported malfunction of the device has been caused by unsuitable hardware, software, installation or operation, devolo reserves the right to charge the purchaser for the resulting testing costs.

6 Additional regulations

The above conditions define the complete scope of devolo's legal liability.

a) The warranty gives no entitlement to additional claims, such as any refund in full or in part. Compensation claims, regardless of the legal basis, are excluded. This does not apply if e.g. injury to persons or damage to private property are specifically covered by the product liability law, or in cases of intentional act or culpable negligence.

b) Claims for compensation of lost profits, indirect or consequential detriments, are excluded.

c) devolo is not liable for lost data or retrieval of lost data in cases of slight and ordinary negligence.

d) In the case that the intentional or culpable negligence of devolo employees has caused a loss of data, devolo will be liable for those costs typical to the recovery of data where periodic security data back-ups have been made.

e) The warranty is valid only for the first purchaser and is not transferable.

f) The court of jurisdiction is located in Aachen, Germany in the case that the purchaser is a merchant. If the purchaser does not have a court of jurisdiction in the Federal Republic of Germany or if he moves his domicile out of Germany after conclusion of the contract, devolo's court of jurisdiction applies. This is also applicable if the purchaser's domicile is not known at the time of institution of proceedings.

g) The law of the Federal Republic of Germany is applicable. The UN commercial law does not apply to dealings between devolo and the purchaser.

Index

C
CE declaration 51
Control lamps 13
D
DHCP server 24
Disposal of old devices 52
dLAN 200 AV network 43
dLAN encryption 25
dLAN password 25
F
Factory default password 46
G
Generate secure password 46
I
Important safety instructions 51
Integrating the new adapter into the network 47
IP address 24
L
LAN (Network connection) 15
Linux 16
M
MAC address 33
Mac OS X 16
N
Network password 46
P
Package contents 12
R
Reset 14
S
Security ID 13, 46
Software installation 15
SSID 30
Standard WLAN key 13, 29
System requirements 12
T
Time server 26
U
Ubuntu 16
W
Warranty 52
WEP 30
Wi-Fi Protected Setup (WPS) 14, 35
Windows 15
WLAN antenna 15
WLAN filter 32
WLAN ON/OFF button 13
WLAN time control 34
WPA 30
WPA2 30